

United States District Court

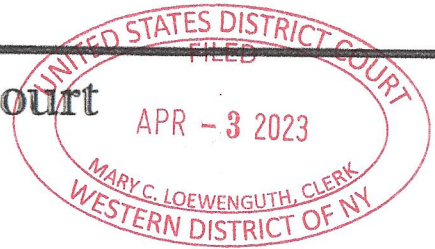
for the
Western District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

The Premises Known as 20 Ferguson Avenue, Buffalo, New York 14213

23-MJ-5041



APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person and property (*identify the person or describe the property to be searched and give its location*):

the Premises Known as 20 Ferguson Avenue, Buffalo, New York 14213, more fully described in Attachment A, which is attached hereto and incorporated by reference herein, located in the Western District of New York, there is now concealed (*identify the person or describe the property to be seized*):

Evidence, contraband, fruits, and instrumentalities pertaining to violations of Title 18, United States Code, Sections 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy), 1343 (Fraud by Wire), 1344 (Bank Fraud), 1349 (Wire Fraud and Bank Fraud Conspiracy), 1028A (Aggravated Identity Theft), 1956(a)(1)(A)(i) (Promotional Money Laundering), 1956(a)(1)(B)(i) (Concealment Money Laundering), 1957 (Transactional Money Laundering), 1956(h) (Money Laundering Conspiracy), 1030 (Computer Fraud and Abuse Act); 471 (Counterfeiting United States Currency); 473 (Buying, Selling, and Transferring Counterfeit United States Currency); Title 21, United States Code, Sections 844 (Simple Possession of Controlled Substances); 841(a)(1) (Distributing, Manufacturing, and Possessing with Intent to Distribute Controlled Substances); and 846 (Conspiracy to Violate 21 U.S.C. § 841(a)(1)), as more fully set forth in Attachment B, which are attached hereto and incorporated by reference herein.

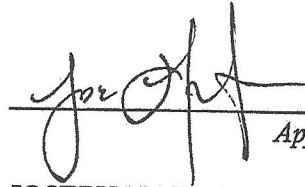
The basis for search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18, United States Code, Sections 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy), 1343 (Fraud by Wire), 1344 (Bank Fraud), 1349 (Wire Fraud and Bank Fraud Conspiracy), 1028A (Aggravated Identity Theft), 1956(a)(1)(A)(i) (Promotional Money Laundering), 1956(a)(1)(B)(i) (Concealment Money Laundering), 1957 (Transactional Money Laundering), 1956(h) (Money Laundering Conspiracy), 1030 (Computer Fraud and Abuse Act); 471 (Counterfeiting United States Currency); 473 (Buying, Selling, and Transferring Counterfeit United States Currency); Title 21, United States Code, Sections 844 (Simple Possession of Controlled Substances); 841(a)(1) (Distributing, Manufacturing, and Possessing with Intent to Distribute Controlled Substances); and 846 (Conspiracy to Violate 21 U.S.C. § 841(a)(1))

The application is based on these facts:

- ☒ continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



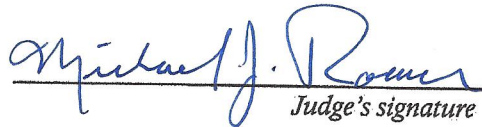
Applicant's signature

JOSEPH NAYLOR
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Printed name and title

Sworn to and signed telephonically.

Date: April 3rd, 2023



Judge's signature

City and state: Buffalo, New York

HONORABLE MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

Printed name and Title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE
41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Joseph Naylor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 20 Ferguson Avenue, Buffalo, New York 14213, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.
2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since July 2022. I am currently assigned to the Cyber Squad, Buffalo Division, in Buffalo, New York, where I work on investigations relating to criminal and national security cyber intrusions. I received my Bachelor's in Finance and my Master's in Information Systems. Prior to becoming an FBI Special Agent, I worked in the private sector, including working in the cybersecurity, information technology and the financial sectors. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.
3. My work in the FBI, as well as the training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against
4. This affidavit is based upon information supplied to me by other law enforcement officers, including other special agents employed by the FBI. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this seizure warrant application.
5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1028(a)(7) (possession

of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy), 1343 (Fraud by Wire), 1344 (Bank Fraud), 1349 (Wire Fraud and Bank Fraud Conspiracy), 1028A (Aggravated Identity Theft), 1956(a)(1)(A)(i) (Promotional Money Laundering), 1956(a)(1)(B)(i) (Concealment Money Laundering), 1957 (Transactional Money Laundering), 1956(h) (Money Laundering Conspiracy), 1030 (Computer Fraud and Abuse Act); 471 (Counterfeiting United States Currency); 473 (Buying, Selling, and Transferring Counterfeit United States Currency); Title 21, United States Code, Sections 844 (Simple Possession of Controlled Substances); 841(a)(1) (Distributing, Manufacturing, and Possessing with Intent to Distribute Controlled Substances); and 846 (Conspiracy to Violate 21 U.S.C. § 841(a)(1)) have been committed by Wul Chol ("CHOL"), who resides at the PREMISES, and others.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

6. Since August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market.¹ Genesis Market is primarily hosted at the Internet domain "genesis.market."² Genesis

¹ In Attachment B, Genesis Market is referred to "Web Market A." At this time, Genesis Market remains active and disclosure of the name of the market would potentially alert its operators of law enforcement action being taken against the users and operators. This may prompt users of the market to notify others of law enforcement action, flee, and/or destroy evidence. Accordingly, the government will file a separate motion to seal the warrant affidavit.

² A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website "g3n3sis.org," as well as the TOR domain "genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxisteprx2qd.onion." TOR is short for "The

Market's operators compile stolen data (e.g., computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected³ computers around the globe and package it for sale on the market.⁴ Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.⁵

7. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts ("resources") associated with the package (e.g., accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc. are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a "fingerprint" associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (i.e., an Internet browser extension that provides additional

Onion Router" and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user.

³ Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

⁴ Genesis Market refers to these packages of stolen data as "bots" on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market's use of the word "bot" strays from the normal meaning, the term "package" is used throughout this request.

⁵ See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at <https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/> (last visited 3/30/23).

functionality). This proprietary plugin amplifies that purchaser's ability to control and access the package's data and masquerade as the victim device.

8. Genesis Market's operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

9. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then requests the new user to associate their Jabber ID⁶ or email address with that new account. Analysis by law enforcement has found that a Jabber ID or email address is not absolutely required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

10. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a "dashboard" of information, including the

⁶ Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

number of packages listed for sale and a “Genesis Wiki” page that walks a new user through Genesis Market’s platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.⁷ The front page displays the total amount of “bots” (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

⁷ Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

genesis

Dashboard Home

Genesis Wiki

News

Bots

Generate FP

Orders

Purchases

Payments

Tickets

Software

Profile

Invites

Logout

Have insider info about Genesis market related investigations? Write us, we are interested.

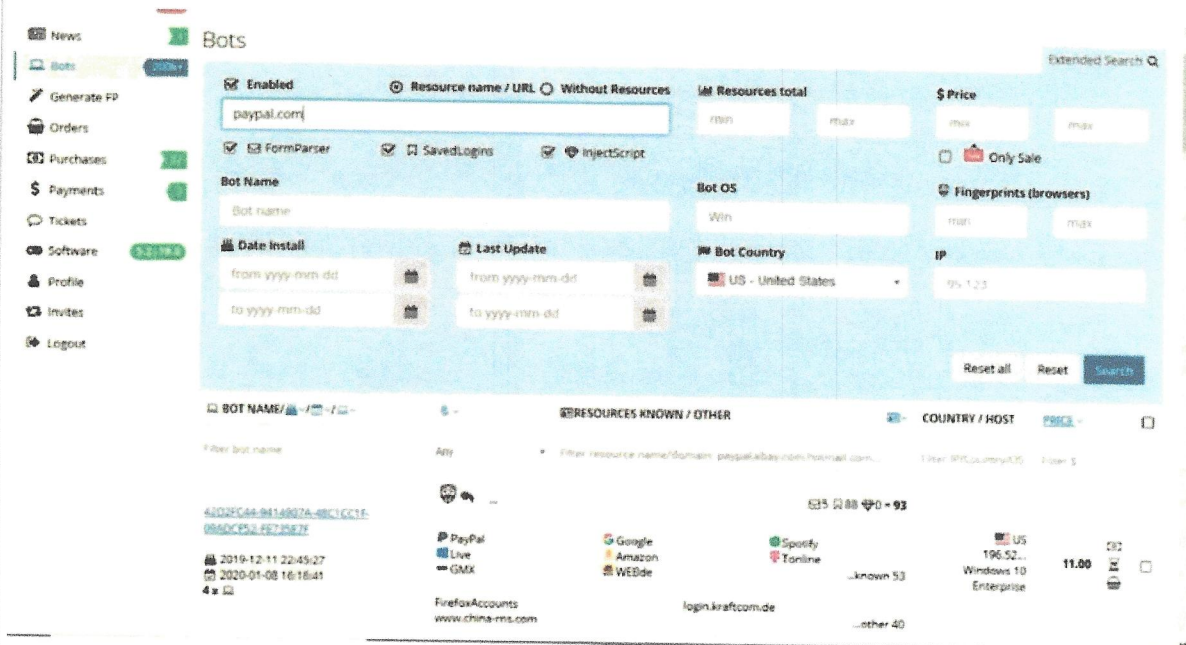
Available Bots

COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall	+22	+4210	+25476	272326
Grouped by				
US	+3	+477	+1388	13625
IT	+2	+557	+2878	52196
FR	+3	+345	+2018	38074
ES	+1	+314	+1931	33329
PL	+1	+305	+1826	14694
AR	+1	+258	+1795	11532
RO	+4	+320	+1648	17309
PT		+177	+1154	22978
CL		+180	+1141	6050
HU		+156	+943	9353
GR		+148	+793	5969
NP		+91	+676	5553
NL	+1	+115	+668	7537
CA		+92	+640	2688
BG	+1	+87	+539	4473
BE		+96	+405	6837
SK		+59	+375	2822
AU		+48	+364	3127
SE	+2	+56	+363	4871
HR		+74	+340	2558
GE		+58	+320	1327

more 126

11. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (e.g., banking information, social media accounts, etc.), country of origin, price,

and the date of infection (*i.e.*, the date the victim device was infected with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:






12. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee's purchase of a Genesis Market package:



13. Below is a screenshot dated November 22, 2019, relating to the same victim package as above, showing the email addresses and passwords (both of which are redacted for the purposes of this affidavit) that are provided to the purchaser of the victim package:

Last update Saved Logins: 2019-11-22 08:55:29
 Last update Form Parser: 1970-01-01 00:00:00
 Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL / LOGIN / PASSWORD / ...	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
https://www.viewerlabs.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	
EA054293-E544B574-B4E249CA-23041EFB-5E465696  SonyEntertainmentNetwork https://accounts.sonyentertainmentnetwork.com/register *Login*: [REDACTED]@gmail.com *Password*: [REDACTED]	Any	Any	Any	Any	

14. When users have questions or issues with Genesis Market, they can submit “tickets” via a “Ticket” tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

15. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.⁸ Before a purchase can be made, however, the user must first deposit a sum of virtual currency into their Genesis Market account. This is done through the “Payments” tab on the Genesis Market website, wherein the user can choose the type of virtual currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.⁹ Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

16. As of October 17, 2022, there were approximately 450,000 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device. According to Genesis Market’s website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

17. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market. Through

⁸ Virtual currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

⁹ Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, the identity of which is known to law enforcement and known to be associated with criminal activity, to process the virtual currency transactions.

these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market operators through the "Ticket" function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims' personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

18. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as "Database A"). The database included, among other things, Genesis Market's administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

19. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

20. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

21. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as "Database B"). The database included the same types of information described above, including information from more than 55,000 Genesis Market user accounts.

CHOL's Activity on Genesis Market

22. The Genesis Market data showed that, from June 13, 2019 to May 10, 2022, a user whose account name was connectgcross ("CONNECTGCROSS") purchased 21 packages on Genesis Market that included 778 stolen account credentials. The registration data for CONNECTGCROSS showed the account was created on June 13, 2019, listed a Jabber ID of connectgcross@jabber.com and showed CONNECTGCROSS deposited \$105.08 to their marketplace account.

23. FBI Milwaukee identified CHOL as a Genesis Market user through legal process to the cryptocurrency exchange Coinbase for a virtual currency transaction used to fund Genesis Marketplace account CONNECTGCROSS from a Coinbase account ("COINBASE ACCOUNT 1"). Coinbase provided records for COINBASE ACCOUNT 1 that listed the owner as "Wul Chol" with 20 FERGUSON AVE, BUFFALO, NY 14213 ("20 FERGUSON") as the customer's address. Coinbase provided Know Your Customer ("KYC") information, which included photographs of CHOL's New York State Identification Card.

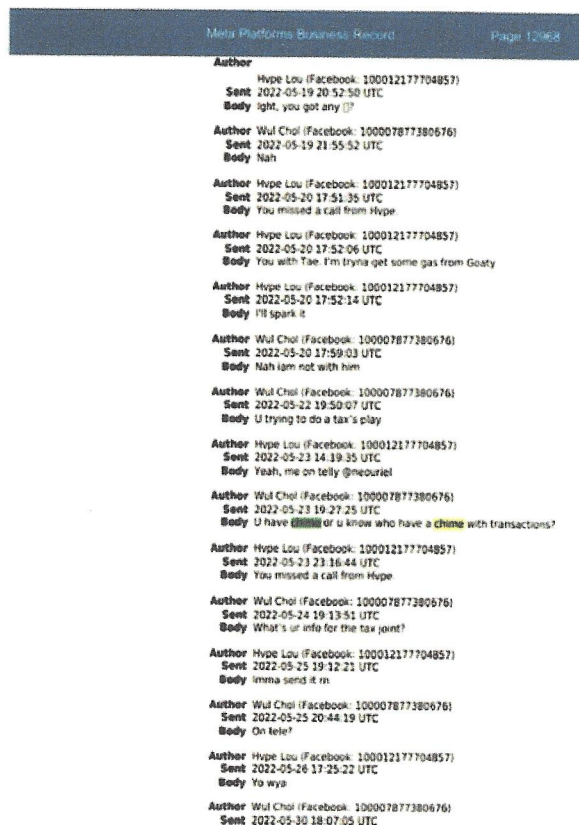
24. CHOL used Internet Protocol (IP) address 192.135.227.228 to access Genesis Marketplace on the following dates: June 17, 2019, June 18, 2019, and July 19, 2019.. CHOL used the same IP address, 192.135.227.228, to access his Coinbase account on the following dates: May 29, 2019, May 31, 2019, June 2, 2019, June 9, 2019, June 10, 2019, and June 28, 2019. Finally, CHOL used the

same IP address, 192.135.227.228, to access Facebook on June 22, 2019. IP address 192.135.227.228 connected to Facebook, Coinbase and Genesis during the same time period. This shows that the same internet connection logged on to all three servers during the same time period. Additionally, the connection to these servers requires authentication, consisting of CHOL's username and password/code in order to log into the server.

25. The IP address 192.135.227.228 comes back to the Buffalo & Erie County Public Library at 1 Lafayette Square, Buffalo, NY 14203. Information from Chol's Facebook account, which is described in more detail below, shows that Chol went to the library on multiple days that correspond with the activity described in the prior paragraph.

- a. On June 2, 2019 at 3:49PM Eastern Time zone CHOL asked another Facebook user to pick him up from the library. CHOL's Coinbase account was also accessed from the Buffalo & Erie County Public Library IP 192.135.227.228 on June 2, 2019 at 2:42PM Eastern Timezone, just over an hour earlier.
- b. On June, 9 2019 CHOL informed another Facebook user that he was going to the library. On June 9, 2019 the Buffalo & Erie County Public Library IP 192.135.227.228 logged into CHOL's Coinbase account at 8:19PM.
- c. On June 12, 2019 CHOL stated in a Facebook conversation at 3:48PM Eastern that he was going to arrive at the library at 4:30PM that day, during normal business hours.
- d. On June 18, 2019 another Facebook user asked CHOL where he was, to which CHOL responded "Library." Also on June 18, 2019 CHOL logged into the Genesis Market from the Buffalo & Erie County Public Library IP address of 192.135.227.228.

- e. On June 26, 2019 another Facebook user asked CHOL where he was, to which CHOL responded "Library."
- f. On June 29, 2019 CHOL informed another Facebook user that he was at the library.



26. On or about November 16, 2022 FBI Buffalo conducted open source social media research and located a Facebook account in the name "Wul Chol", with the Facebook username wul.chol.1 ("TARGET ACCOUNT") and Facebook User ID 100007877380676. Further research into TARGET ACCOUNT confirmed the account's connection to CHOL.

27. On December 19, 2022, based on publicly viewable evidence of criminal activity on TARGET ACCOUNT, the Honorable Jeremiah J. McCarthy, Magistrate Judge for the Western District of New York, signed a Search Warrant to Facebook associated with the TARGET ACCOUNT. The search warrant allowed agents to search for evidence of violations of Title 18, United States Code, Sections 1343 (Fraud by Wire), 1349 (Wire Fraud Conspiracy), 1028A (Aggravated Identity Theft), 1956(a)(1)(A)(i) (Promotional Money Laundering), 1956(a)(1)(B)(i) (Concealment Money Laundering), 1957 (Transactional Money Laundering), 1956(h) (Money Laundering Conspiracy) and 1030 (Computer Fraud and Abuse Act).

28. On January 11, 2023 Facebook responded to the Search Warrant and returned the requested data for the time period June 1, 2019 to December 19, 2022. On or about January 31, 2023 investigators began analyzing the data in the Facebook return, to search for evidence of violations of the statutes identified in the search warrant. Upon initial review, and while searching for such evidence, investigators discovered evidence of additional criminal violations beyond those identified in the original search warrant. The data showed evidence of drug possession, drug distribution and the use of electronic communication methods to facilitate drug distribution. Due to the discovery of the additional evidence agents applied for an Amended Search Warrant to search for evidence of violations of Title 21, United States Code, Sections 844 (Simple Possession of Controlled Substances); 841(a)(1) (Distributing, Manufacturing, and Possessing with Intent to Distribute Controlled Substances); and 846 (Conspiracy to Violate 21 U.S.C. § 841(a)(1)). On February 10, 2023 the Honorable H. Kenneth Schroeder, Jr., Magistrate Judge for the Western District of New York, signed the Amended Search Warrant.

29. A review of search warrant returns for the TARGET ACCOUNT revealed evidence of a variety of illegal activities, which are summarized below.

30. On March 10, 2020 CHOL had a Facebook Messenger ("MESSENGER") conversation with GTG. The conversation discussed counterfeit money. In this conversation, which is shown in Exhibit 2 below, CHOL discussed receiving counterfeit twenty dollar bills, from an individual identified as Milly. CHOL stated that the counterfeit money Milly provided was of poor quality. CHOL also referred to an accomplice known as Ed who attempted to use counterfeit money to purchase a cashier's check. CHOL stated that he would "cop giftys", which based on my training and experience means he would use the counterfeit money to purchase gift cards. CHOL then asked GTG if he knew of a place to cash the gift cards that were purchased with counterfeit money, to which GTG stated that he does.

Exhibit 2

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:51:17 UTC
Body: Ed can get off with his tip he told me

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:51:48 UTC
Body: Is cause he doing it the dumb way [TEXT]

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:52:20 UTC
Body: Fakes I told u got to get up a model that is a corner at a store

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:52:40 UTC
Body: I got 2 [TEXT]

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:52:51 UTC
Body: But the 20s Milly gave you not that good she print them bad

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:53:39 UTC
Body: She was supposed to make them 20s a little darker 20s at a common like he should get 50s

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:53:44 UTC
Body: My rigga it's not real otherwise they got look bad compared to real money

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:53:53 UTC
Body: Is

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:54:17 UTC
Body: I was using 1k in 50s & 500 in 20s

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:54:40 UTC

Meta Platform Business Review Page 36/47

Body
Is but she got some 20s that is good too but the ones she gave Ed look bad

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:55:00 UTC
Body: Dam

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:55:12 UTC
Body: He tried off into 2 [TEXT]

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 12:55:38 UTC
Body: Is but if its me is going to a cashier that look nonchalant and cop giftys he went to 711 and he still tried to cop of a tricked cashier that's white

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 12:58:28 UTC
Body: [TEXT]

Author: Wul Choi (Facebook: 100007877380676)
Sent: 2020-03-10 13:02:02 UTC
Body: U found a place to cash the giftys out

Author: Tazir Qig (Facebook: 100008893965036)
Sent: 2020-03-10 13:02:39 UTC
Body: Now but this Somalian dude is know where

31. On April 22, 2020 CHOL had a MESSENGER conversation with GTG. The conversation discussed an online shopping scam. CHOL asked GTG “Can u check my page gout telling me I got a ham and see what she did cuz gout telling me he mobile and other shit”. Based on my training and experience, CHOL asked GTG to check a fraudulent webpage, in which CHOL played some role, that markets itself as selling shoes. The apparent purpose of this page was to solicit customers to purchase shoes, however, based on the chat described below, CHOL did not appear to have any intention of selling shoes to the customer. The potential customers were referred to as “hams”. In the screenshot, labeled Exhibit 3, CHOL told GTG to charge the customer \$650 (which CHOL later changed to \$850), for shoes that the customer was inquiring about. Exhibit 4, a screen capture from GTG’s phone, showed a message from the victim of the scam to GTG. GTG was logged into the CHOL’s store that is offering to sell shoes, and was discussing the shoes that the victim wants to purchase. In Exhibit 5 CHOL had a conversation with PAPE in which CHOL asked PAPE to use PAPE’s Instagram pages to comment on CHOL’s “ham” Instagram page and state that PAPE received tracking and paid through CashApp. This behavior provides probable cause to believe that CHOL did not have any intention on sending shoes to customers.

Exhibit 3

Meta Platforms Business Record Page 9852

Body
To

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:13:21 UTC
Body To

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:19:17 UTC
Body To

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:21:03 UTC
Body Can u check my page gout telling me I got a ham and see what she did cuz gout telling me he mobile and other shit

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:21:32 UTC
Body right cause someone sent your ham thier zelle

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:21:46 UTC
Body Though it was you

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:22:07 UTC
Body Nah she replying

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:23:05 UTC
Body U got data

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:23:07 UTC
Body For pics?

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:23:16 UTC
Body She want the desert sage and zebra

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:23:21 UTC
Body And I'm taking ya my ham

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:24:04 UTC
Body Nah my point finsh when she was hitting me up at like 5 and I can only use Facebook free

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:26:15 UTC
Body right

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:26:28 UTC
Body U got me tho

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:27:29 UTC

Meta Platforms Business Record Page 9853

Body
Text her ya prices tho

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:27:45 UTC
Body ima sendthe pics

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:27:50 UTC
Body U herd

Author Wu Chol (Facebook: 100007877380676)
Sent 2020-04-22 02:28:57 UTC
Body For all three say 650 but I can't I can only talk on Facebook and Facebook free I cant even see pics on face book

Author Tazz Gtg (Facebook: 100008893965036)
Sent 2020-04-22 02:29:06 UTC
Body Tazz sent a photo.

Attachments image-2592857297642684 (2592857297642684)
Type image/png
Size 46208
URL https://interncache-nao.fscdn.net/v/t1.15/52-9/94030611_2592857304309350_4320520260918444032_n.jpg?ccb=1-7&nc_sid=73a6a0&efg=eyJ1cm90ZW40OjwyaH9fdXN2VWxZVWZNaWVudC90bW9nZW40M8j7TWVwVWV0Gncyj9&nc_ad=2-m6_nc_sid=0&nc_ht=interncache-nao&oh=03_AdQ4wjaVH9mrfzInYXC13imUvCvsr6yDofwyQ9trRA6oe=63E6840E

Exhibit 4

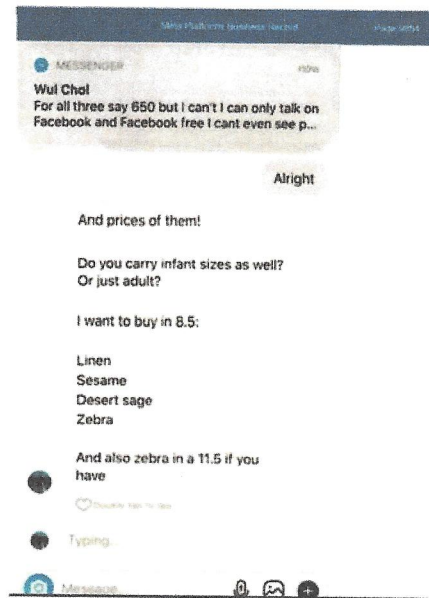


Exhibit 5

Meta Platforms Business Record Page 1244

Body
U flipped ur firs

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-09 17:19:55 UTC
Body ?

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-03-09 20:28:11 UTC
Body Yo

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-03-09 21:44:33 UTC
Body Lol got me on tele

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-05-06 15:15:24 UTC
Body Yo u got any other insta pages thats u dont use

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:27:14 UTC
Body Yea

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:27:29 UTC
Body U tryna turn it to a ham page ?

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-05-06 15:32:47 UTC
Body Nah iam trying to so fake comments like I just received tracking and I paid through cash app and he legit like that

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:33:31 UTC
Body What's your page? & that page got like 7 followers

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:33:52 UTC
Body I did that before too lmao

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-05-06 15:34:20 UTC
Body Follow more people its forever_drip

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:35:46 UTC
Body U had hammet doin u funny asf [REDACTED]

Author Stack Pape (Facebook: 100006949933414)
Sent 2020-05-06 15:36:09 UTC
Body Ight imma comment on them lmao

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-05-06 15:36:59 UTC
Body Hell yea bra I need that bread

Author Wul Chol (Facebook: 100007877380676)
Sent 2020-05-06 15:38:14 UTC
Body Any way

32. On June 13-14, 2022 CHOL had a MESSENGER conversation with Robert Sardo ("SARDO"). The conversation discussed the sale of a controlled substance. SARDO contacted CHOL and informed him that he needs to purchase 30 "xans", which based on my knowledge and experience

refers to the controlled substance Alprazolam¹⁰. CHOL and SARDO then arrange to meet in person for the exchange. The conversation can be seen in Exhibit 6 below.

Exhibit 6

Meta Platforms Business Record
Page 13236

Author Manando Wu (Facebook: 100030015379407)

Sent 2022-10-30 19:25:15 UTC

Body Okay no problem

Author Manando Wu (Facebook: 100030015379407)

Sent 2022-10-30 19:26:28 UTC

Body If God is willing you will make it

Thread (325064004518543)

Current 2022-11-16 17:35:33 UTC

Participants Robert Sardo (Facebook: 100015471428239)

Wul Choi (Facebook: 100007877380676)

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-13 23:59:18 UTC

Body Yo I need like 30 xans

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 00:00:30 UTC

Body Robert called you.

Call Record Missed false

Duration 31

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-06-14 01:15:06 UTC

Body Yo what time pull up?

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 01:17:33 UTC

Body I'm stw home rn from work is there way u can pull up on me or i got to come to you

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 01:21:18 UTC

Body You missed a call from Robert.

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 01:21:32 UTC

Body ?

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 01:24:42 UTC

Body Robert called you.

Call Record Missed false

Duration 50

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-06-14 01:33:47 UTC

Body My ride is stw i'm jumpin the shower

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-06-14 01:43:08 UTC

Body Ok bet

Author Robert Sardo (Facebook: 100015471428239)

¹⁰ Alprazolam, which is sold under the brand name Xanax, is a Schedule IV controlled substance.

Meta Platforms Business Record		Page 13237
Sent		
2022-06-14 02:13:43 UTC		
Body	Robert called you	
Call Record	Missed	false
Duration 1		
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:14:23 UTC		
Body	Robert called you	
Call Record	Missed	false
Duration 32		
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:31:51 UTC		
Body	Robert called you	
Call Record	Missed	false
Duration 10		
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:32:59 UTC		
Body	Grey car	
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:35:15 UTC		
Body	You missed a video chat from Robert.	
Author Wui Choi (Facebook: 100007877380676)		
Sent 2022-06-14 02:36:04 UTC		
Body	You called Robert	
Call Record	Missed	false
Duration 39		
Author Wui Choi (Facebook: 100007877380676)		
Sent 2022-06-14 02:40:12 UTC		
Body	You called Robert	
Call Record	Missed	false
Duration 15		
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:42:34 UTC		
Body	Robert called you	
Call Record	Missed	false
Duration 15		
Author Robert Sardo (Facebook: 100015471428239)		
Sent 2022-06-14 02:43:34 UTC		
Body	You missed a call from Robert	
Author Wui Choi (Facebook: 100007877380676)		
Sent 2022-06-14 02:44:11 UTC		
Body	You called Robert	
Call Record	Missed	false
Duration 16		
Author Wui Choi (Facebook: 100007877380676)		
Sent 2022-06-14 04:29:46 UTC		
Body	Robert missed your call	
Author Robert Sardo (Facebook: 100015471428239)		

33. On August 6, 2022 CHOL had a MESSENGER conversation with SARDO. The conversation discussed the purchase of marijuana through an illegal online marketplace on the messaging application Telegram¹. In the conversation CHOL sent the website address for “Premium Exotics” (<https://t.me/premiumexotics32>), to SARDO and stated, “They got some good gas for the low bro”. Based on my knowledge and experience “gas” is slang for marijuana. This can be seen in Exhibit 7 below. CHOL then stated that he had purchased from Premium Exotics before and sent a video of marijuana. CHOL then further discussed the pricing of the marijuana. Exhibit 8 is a screenshot from this video which shows a bag of marijuana.¹²

Exhibit 7

Meta Platforms Business Record Page 13244

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-17 23:30:46 UTC
 Body A bull?

Author Robert Sardo (Facebook: 100015471428239)
 Sent 2022-07-17 23:36:13 UTC
 Body Bull

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-18 00:22:59 UTC
 Body Oh right but: already got 1

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-28 21:01:02 UTC
 Body U know anyone with accounts trying to make bread?

Author Robert Sardo (Facebook: 100015471428239)
 Sent 2022-07-30 04:45:11 UTC
 Body Where the xang at

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-30 18:19:35 UTC
 Body U know anyone with boar?

Author Robert Sardo (Facebook: 100015471428239)
 Sent 2022-07-30 18:23:40 UTC
 Body What that

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-30 18:25:59 UTC
 Body Bank of America

Author Robert Sardo (Facebook: 100015471428239)
 Sent 2022-07-30 18:28:32 UTC
 Body Ahh

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-30 18:29:07 UTC
 Body Tea

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-07-31 18:52:52 UTC
 Body U know anyone with bank accounts

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-08-06 21:49:19 UTC
 Body <https://maipremiumexotics32>
 Share Date Created: 2022-08-06 21:49:18 UTC
 Summary Good exotics for good prices
 Title Premiumexotics
 URL <https://maipremiumexotics32>

Author Wu/Chel (Facebook: 100007877380676)
 Sent 2022-08-06 21:49:33 UTC
 Body They got some good gas for the low ans

Author Robert Sardo (Facebook: 100015471428239)

Meta Platforms Business Record

Page 11246

Sent

2022-08-06 22:47:37 UTC

Body Say less

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-08-06 23:06:13 UTC

Body Join the channel

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:06:32 UTC

Body Idk how

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-08-06 23:16:11 UTC

Body U got telegram?

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:16:17 UTC

Body Nah

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:16:26 UTC

Body I feel they scamming right?

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-08-06 23:19:29 UTC

Body Nah u got to know who vouched i vouch for them they fuck with me

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-08-06 23:20:11 UTC

Body Got this from them

Author Wul Choi (Facebook: 100007877380676)

Sent 2022-08-06 23:20:17 UTC

Body You sent a video.

Attachments video-1659828017.mp4 (596414468737895)

Type video/mp4

Size 4831072

URL https://intercache-ldc.rpcdn.net/v/R42.3356.2/2

97857042.7777328035675162.5659564731186

598711.n.mp4/video-1659828017.mp4?cc=1

76.nc.s=d=060d786efp=ayjLcmxrZW4OjwaH

0f0jgAZ2VhX2NoaWVudC90enRpdHxvWV2c2Fn

ZV92aWRlby96vabr=24153366.nc.fw=ntemc

archoIdc&ch=03_AcQf1OxjQyTekoZ0vKATT

mjFu0Q03qH3tH2XpVg6ce=6376584A&d=1

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:28:02 UTC

Body Reacted ♡ to your message

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:28:10 UTC

Body Det

Author Robert Sardo (Facebook: 100015471428239)

Sent 2022-08-06 23:28:14 UTC

Meta Platforms Business Record Page 13246

Body
What is it?

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-06 23:28:17 UTC
Body Hm

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-06 23:30:52 UTC
Body It was black cherry gelato for \$250 for 2 ounces

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-06 23:31:01 UTC
Body Word

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-06 23:31:04 UTC
Body Imma fuck wit em

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-06 23:36:11 UTC
Body Yes they got some ps for like 700

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-09 18:33:37 UTC
Body Robert missed your call

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-09 19:09:18 UTC
Body Yo

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-09 19:16:55 UTC
Body U knew who got boe we going to get this bread easy with out a doubt

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-09 19:17:12 UTC
Body Robert missed your call

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-09 21:14:54 UTC
Body Robert missed your call

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-09 21:19:55 UTC
Body You missed a call from Robert

Author Wul Chel (Facebook: 100007877380676)
Sent 2022-08-09 21:50:10 UTC
Body You called Robert

Call Record Missed false
Duration 167

Author Robert Sardo (Facebook: 100015471428239)
Sent 2022-08-12 21:10:35 UTC
Body U got kans

Author Wul Chel (Facebook: 100007877380676)

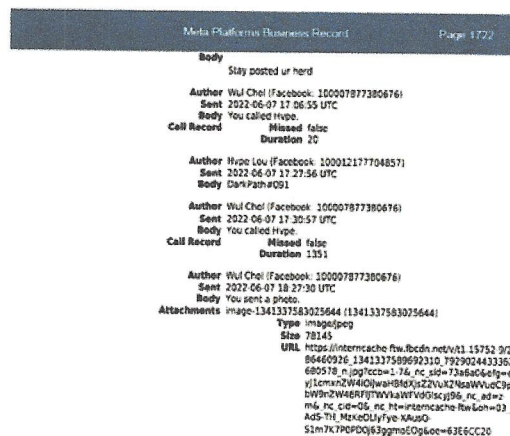
Exhibit 8

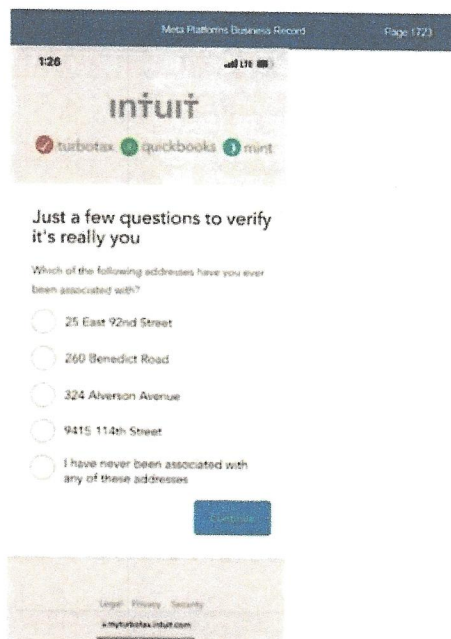


34. On May 22, 2022 to August 23, 2022 CHOL had a MESSENGER conversation with “LOU”. The conversation discussed potential tax fraud. In the conversation CHOL asked LOU, “U trying

to do a tax's play"? LOU agreed and asked CHOL to contact him on Telegram. CHOL and LOU then began to discuss the tax fraud again on MESSENGER on June 3, 2022. On June 7, 2022 CHOL began to fill out an Intuit TurboTax form based on LOU's information, including asking LOU for various personal identifiers (see Exhibit 9 below). On August 18, 2022 CHOL informed LOU that he needs to make an appointment with the IRS to get the money (see Exhibit 10).

Exhibit 9





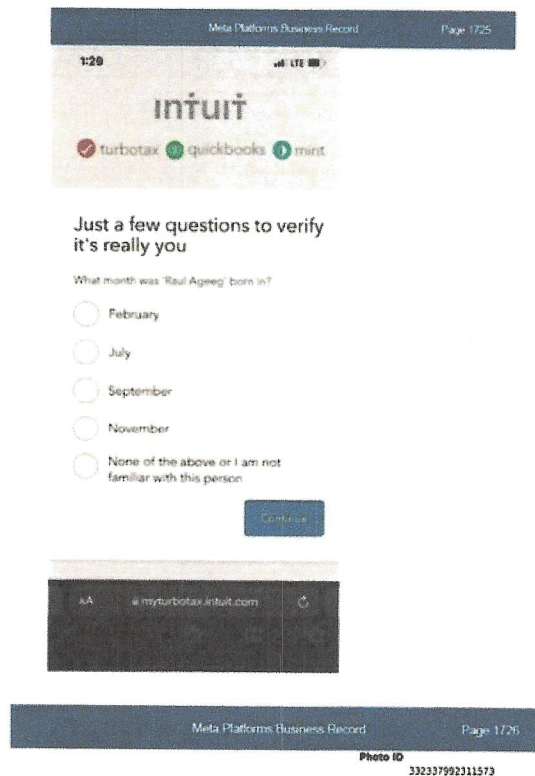
Author Hype Lou (Facebook: 100012177704857)
 Sent 2022-06-07 18:28:27 UTC
 Body None of the addresses

 Author Wul Chel (Facebook: 100007877380676)
 Sent 2022-06-07 18:28:30 UTC
 Body Hype missed your call.

 Author Hype Lou (Facebook: 100012177704857)
 Sent 2022-06-07 18:29:13 UTC
 Body You missed a call from Hype

 Author Wul Chel (Facebook: 100007877380676)
 Sent 2022-06-07 18:29:28 UTC
 Body I am text u if it's more questions

 Author Wul Chel (Facebook: 100007877380676)
 Sent 2022-06-07 18:30:15 UTC
 Body You sent a photo.
 Attachments image:332337992311573 (332337992311573)
 Type image/jpeg
 Size 71213
 URL https://intencache-flw.fbcdn.net/v/t1.15752-9/285797777_332337995644906_3054307645205215779_n.jpg?ccb=1-7&nc_sid=73af6a06efg=eyJ1cm90Zm44OjwyaW90dXJlZGVuZ2N5aWZlbnVudC9pbW9nZW46NjU1VWVkaWV0dG90cy90&nc_gid=m6_nc_id=06_nc_h=intencache-flw6oh=03_AdTTTgrvSjlmkXiaShNPVZHQY2MAp_k0pwisMZGs_eMReOGoe=63E68257

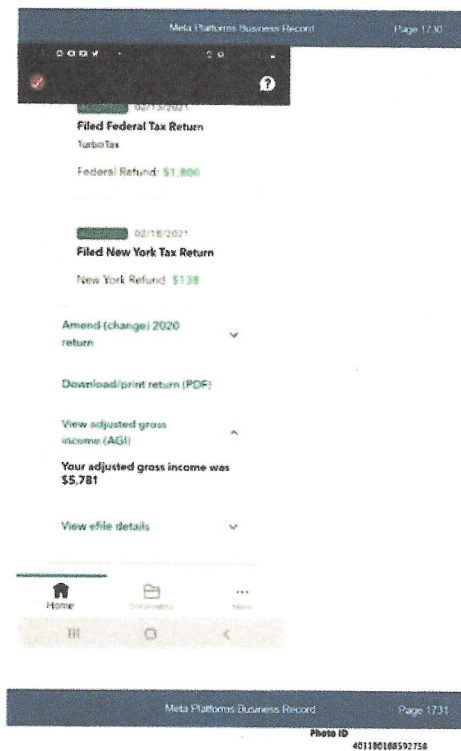


Author Hype Lou (facebook: 100012177704057)
Sent 2022-06-07 18:30:51 UTC
Body September

Author Wul Chol (facebook: 100007877380676)
Sent 2022-06-07 18:32:21 UTC
Body You sent a photo.

Attachments image: 541906060730904 (541906060730904)
Type image/jpeg
Size 94156
URL https://interncache.ftw.ftcdn.net/v1/1.15752.9/2/06166644.5419060606404237_5060512989862035693?n=pg7ccc=1-7&nc_sid=13a6a0&elp=eyJlcmxwZW44Ojwa48MDkxZ2VxX2NsaWVudC9pbW9kZW46RjIjTWVkaWV0Giscy9k,nc_ad=2 m&nc_cid=55,nc_ht=interncache.ftw.ftcdn=03_AdR08BUA2n0OCrpkMsscYCBepbe9ZYNbwgbrgKeG352ju06oe=63CE68DF1

29



Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-08 18:17:47 UTC
 Body I have a high credit score?
 Author Hupe Lou (Facebook: 100012177704857)
 Sent 2022-06-08 18:41:09 UTC
 Body Nah
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-08 18:53:25 UTC
 Body What's ur score?
 Author Hupe Lou (Facebook: 100012177704857)
 Sent 2022-06-08 19:01:38 UTC
 Body 500 something I got a debt from t mobile
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-08 19:22:43 UTC
 Body Damn right
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-09 17:42:43 UTC
 Body Lou make a America First credit union
 Author Hupe Lou (Facebook: 100012177704857)
 Sent 2022-06-14 22:15:32 UTC
 Body Hupe called you
 Call Record Missed /false
 Duration 35
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-15 18:49:33 UTC
 Body Yo
 Author Hupe Lou (Facebook: 100012177704857)
 Sent 2022-06-15 18:51:37 UTC
 Body Yo
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-15 18:58:39 UTC
 Body Why n ?
 Author Hupe Lou (Facebook: 100012177704857)
 Sent 2022-06-16 16:57:39 UTC
 Body Yo
 Author Wu Chel (Facebook: 100007877380676)
 Sent 2022-06-16 17:36:44 UTC
 Body rgt

Exhibit 10

Meta Platforms Business Record		Page 1735
Body	Yo	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-07-31 21:21:40 UTC	
Body	U finish the joint?	
Author	Hype Lou (Facebook: 100012177704857)	
Sent	2022-07-31 21:55:08 UTC	
Body	jays bout to bring my id. i'm bout to go to bandman build	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-07-31 22:01:29 UTC	
Body	ight	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-01 19:09:06 UTC	
Body	Hype missed your call.	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-02 22:25:28 UTC	
Body	Hype missed your call.	
Author	Hype Lou (Facebook: 100012177704857)	
Sent	2022-08-02 22:29:12 UTC	
Body	Hype called you.	
Call Record	Missed false	
	Duration: 45	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-02 22:29:23 UTC	
Body	U still ain't do the idme joint?	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-03 00:52:06 UTC	
Body	Hype missed your call.	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-17 23:12:45 UTC	
Body	Yo	
Author	Hype Lou (Facebook: 100012177704857)	
Sent	2022-08-18 00:27:37 UTC	
Body	Yo	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-18 00:40:31 UTC	
Body	U got to make an appointment with the IRS to get the money	
Author	Wul Chel (Facebook: 100007877380676)	
Sent	2022-08-23 15:46:06 UTC	
Body	You sent a photo.	
Attachments	image:589677322622418 (589677322622418)	
	Type: image/jpeg	
	Size: 111108	
	URL: https://intcache-fre.fcdn.net/vr1.15752-9/301035289_589677322622418_8294140496782768276_n.jpg?ccb=1-7&nc_sid=7386a0&efg=eyJ1cmxhZW40dWwH8dXjs2ZVx2NsaWVudC9pb	

35. On November 27, 2022 to November 30, 2022 CHOL had a MESSENGER conversation with GTG. The conversation discussed wire and/or bank fraud. CHOL sent a guide, in the form of a PDF, to GTG that showed how to manufacture fraudulent money orders to send through Western Union (See Exhibit 11 below). The guide showed a user, step by step, how to change a Western Union money order from one amount (such as \$1.00) to another amount (such as \$1,000). Step 1 of the guide instructed the user to utilize sandpaper to scratch the \$1.00 off the Western Union money order. Step 2 showed the "\$1.00" removed from the money order. Step 3 provided a template that the user would use to print over the area that had been scratched off. Step 4 showed an example of what the template would look like if the user used \$1,000 in the place of the scratched off \$1.00. Step 5 showed the user how to align the

template on the scratched-off money order to ensure that it is printed correctly. Step 6 showed the template and money order taped together. Step 7 showed the user how to load the combined template and money order into a printer. Step 8 showed the finished product. GTG then responded to CHOL and said "Send me the 500 one too", to which CHOL sent a document containing the template to print a \$500.00 money order (see Exhibit 12 below).

Exhibit 11

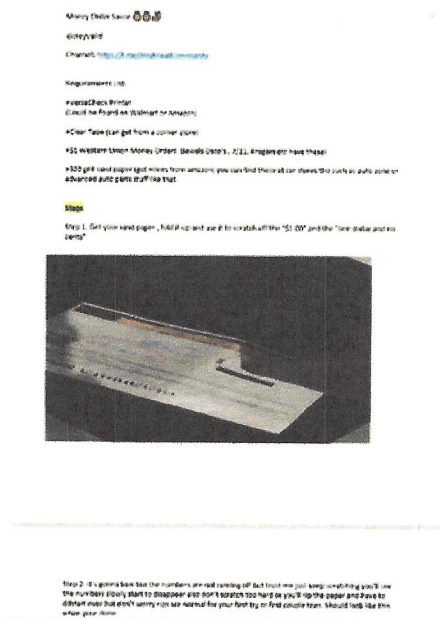


Exhibit 12

500.00

FIVE HUNDRED DOLLARS AND NO CENTS

36. On August 3, 2022 CHOL had a MESSENGER conversation with Duce Deuce. The conversation discussed bank fraud. DEUCE starts the conversation by messaging CHOL and saying "Yea I Hurd Boa hitting." Based on my training and experience DEUCE is referring to Bank of America when he says "BOA", and hitting means that the bank is paying out on fraudulent checks that are being cashed. Furthering the conversation CHOL sent the screenshot below (Exhibit 13) to DEUCE and stated that he, along with another individual, filed taxes for an individual by the name of Tyreke. However, CHOL then stated that Tyreke's mother cancelled the deposit before Tyreke could remove the fraudulent funds. CHOL then stated that he was going to "gather mad heads". Based on my training and experience "heads" refers to individuals that have bank accounts and would allow CHOL to use them for fraudulent purposes. The conversation can be found in Exhibit 14 below.

Exhibit 13

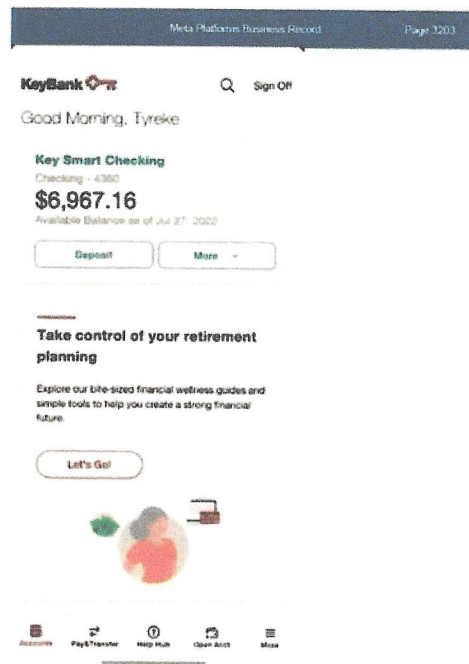


Exhibit 14

Meta Platforms Business Record

Page 3201

Body

Igh then tell him give me a band up front then and i'm down

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:09:39 UTC

Body You missed a call from Duce.

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:10:00 UTC

Body Yo u called?

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:10:20 UTC

Body Yea i Hurd Bea hitting

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:13:23 UTC

Body You missed a call from Duce.

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:16:40 UTC

Body Yea it is

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:16:57 UTC

Body So get my shiz buasing what u waiting for

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:19:20 UTC

Body Bet what's the deposit limit?

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:20:02 UTC

Body U be getting bread to it too?

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:20:14 UTC

Body 25k

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:21:38 UTC

Body Bet that iam hit my grub Man U herd

Author Duce Deuce (Facebook: 100033876159945)

Sent 2022-08-03 00:21:52 UTC

Body Igh

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:22:17 UTC

Body Last week i did a play with him and this happened

Author Wul Chol (Facebook: 100007877380676)

Sent 2022-08-03 00:22:21 UTC

Body You sent a photo.

Attachments image:592015115893557 (592015115893557)

Type image/jpeg

Size 92525

URL https://interncache.fw.fbcdn.net/v/t1.15752-9/296243946_507944102744890_92205580812937

Meta Platforms Business Record

Page 3204

Photo ID

592015115893557

Author Duce Deuce (Facebook: 100033876159945)
Sent 2022-08-03 00:22:48 UTC
Body That's keybank

Author Wul Chol (Facebook: 100007877380676)
Sent 2022-08-03 00:23:49 UTC
Body And the nigga that we dropped it in was acting weird cuz his mom said to cancel it so once the bread was on there he was not replying and his mom closed his joint down with out wiping it

Author Duce Deuce (Facebook: 100033876159945)
Sent 2022-08-03 00:24:25 UTC
Body Bet

Author Wul Chol (Facebook: 100007877380676)
Sent 2022-08-03 00:28:09 UTC
Body Yo and m iam trying to gather mad heads m to get a big pay out

Author Duce Deuce (Facebook: 100033876159945)
Sent 2022-08-03 00:29:01 UTC
Body Wym

Author Wul Chol (Facebook: 100007877380676)
Sent 2022-08-03 00:34:44 UTC
Body Like find more people with accounts and run it up

Author Duce Deuce (Facebook: 100033876159945)
Sent 2022-08-03 00:34:58 UTC
Body Nigga make my check[]

Author Duce Deuce (Facebook: 100033876159945)
Sent 2022-08-03 00:36:51 UTC
Body Duce sent a photo.

Attachments image-363783575941676 (363783575941676)
Type image/jpeg
Size 91269
URL https://interncache-ftw.fbcdn.net/v/t1.15752-9/296296025_363783582608342_1748450699519032325_n.jpg?ccb=1-7&nc_sid=73a6a0&efg=eyJ1cmxhZW4iOiJwaH8fdXIsZ2VuX2NsaWVudC9pbW9nZW46RFljTWVkaWVudGlsYy96_&nc_ad=z-m&nc_cid=06_&nc_ht=interncache-ftw&oh=03_AdOhly1IEVCgMi-HaLu1zqR6EY5M6ZTp7naagjWv1LKwIQ&oe=63E69F98

37. On August 7, 2020 CHOL had a MESSENGER conversation with ("SHIESTY"). This conversation involved credit card fraud. CHOL sent SHIESTY a guide showing how to scam credit cards. A picture showing a page of the guide is shown below in Exhibit 15, and the conversation is shown in Exhibit 16.

Exhibit 15

SAKS METHOD

1. Get a nyc place for faster approval
2. Make sure you don't go over 1k because then it'll be considered to be sent to billing address on card (between 500-1k)
3. Use different names on billing and shipping address. put drop address and put phone # on the cc. For billing address use phone # on cc as well. Have a dummy email with cardholders name already set up
4. Once info is set, move onto ground shipping and always do free. enter card information but don't copy and paste!
5. Wait for order to process y'

Saks.com

1. State CC
2. Debit Classic Card
3. Bill = CC
4. Ship = Drop
5. CC Name On Order & CC Real Phone Number
6. Try 60% Shipment pg

CASHAPP METHOD 1k PER DAY

1. Find somebody who got CashApp & they must have access to their bank or cashapp card to get the cash off but the account must have been active for at least 3 months & have over 10 transactions
2. Log onto univis.com but make sure you got cash on there to buy a card. type in one of yo bins and buy a piece with the feds so you can sign up for cashapp with it which is SSN, bday, etc...
3. Once you buy the card you gone use, type all the full information to sign up under a new cashapp but you gotta make sure you create the account on a different phone, iPhone or android with a VPN Downloaded (OpenVPN)
4. Once you activated the cashapp sign up for a cash card and send it to the address where you want it to land so when it came you can go straight to the ATM & get the cash out or you can use the cash back method entering stores grabbing a small item and getting cash back (the change) for the purchase.
5. If you got someone with cash app & a bank account you can type in the amount you're sending & pay it out to them. Since this is your first payment, I advise not to send nothing over \$500. Over time, you'll be able to send more without any worries as long as the piece is popping.
6. You can do this every 24 hours \$1000+ daily, as soon as you send the cash over to the other cashapps, have the person withdraw it from their bank from the teller make sure not to get it from a ATM or the ATM will keep the card stuck inside.

Exhibit 16

Meta Platforms Business Record Page 148/23

38. On April 13, 2022 CHOL had a MESSENGER conversation with jerry joblins (“JOBLINS”). The conversation discussed the sale of a controlled substance. In the conversation JOBLINS contacts CHOL and asked if he has “gas”. CHOL responded that he doesn’t have gas but has “xans”. CHOL sent Exhibit 17 below to JOBLINS, which was a picture of Alprazolam in a bag. CHOL and JOBLINS made a deal to purchase 10 Alprazolam for \$80.00 and meet in Dewey Park, which was believed to be the park at the intersection of Dewey Avenue and Kensington Avenue in Buffalo, New York. The described conversation can be seen in Exhibit 18 below.

Exhibit 17

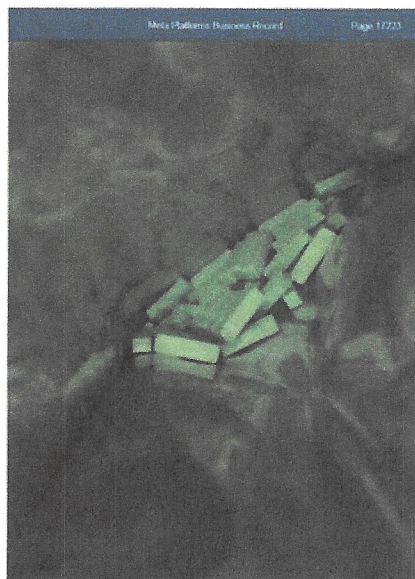


Exhibit 18

Meta-Plasticarum Buxtonii Nakazumi Page 1/222

39

Meta Platforms Business Record

Page 17/224

Photo ID

64667460066356

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-18 21:29:10 UTC
Body Bett Ink when you pull up

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-19 19:22:38 UTC
Body Yo my bad some fuck shit happened yesterday

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 21:01:08 UTC
Body It's alright

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 21:01:24 UTC
Body Meet me here ok?

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 21:01:38 UTC
Body C'Dewey

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-19 22:05:29 UTC
Body light bet

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-19 22:39:49 UTC
Body It's going to be 80 for the 16 u herd

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 22:42:26 UTC
Body Bet

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 23:41:16 UTC
Body Tone

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-19 23:48:01 UTC
Body Yo

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 23:53:02 UTC
Body You there

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-19 23:53:45 UTC
Body You there

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:04:57 UTC
Body Nah not yet

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:15:58 UTC
Body Let me get ur number

Meta Platforms Business Record

Page 17/225

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-20 00:11:45 UTC
Body Why you wait my number

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:12:16 UTC
Body To call when I am outside

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-20 00:13:12 UTC
Body Call me on messenger

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:18:24 UTC
Body light bet

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:32:38 UTC
Body Inuit to there in like 10 min

Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-20 00:32:43 UTC
Body Bet

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:45:16 UTC
Body You called Jerry

Call Record Missed: false
Duration: 25

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:45:18 UTC
Body I am here

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:46:19 UTC
Body At the dead end joint

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:47:42 UTC
Body You called Jerry

Call Record Missed: false
Duration: 50

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:49:33 UTC
Body On Dewey near the snout

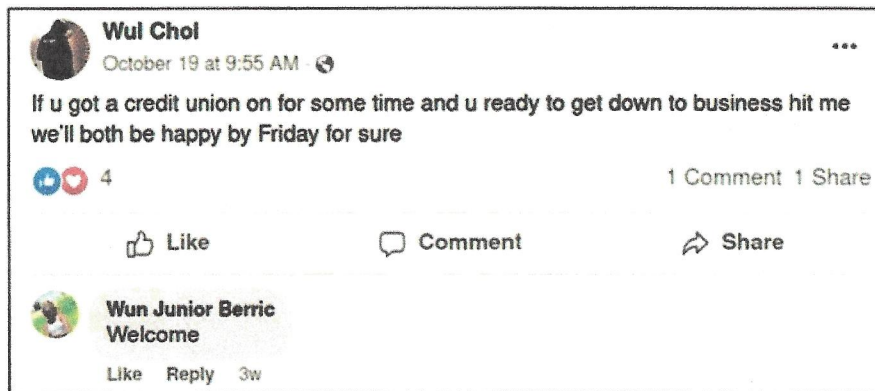
Author Jerry Jobins (Facebook: 100056194737380)
Sent 2022-04-20 00:49:44 UTC
Body Bet! what car

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:50:05 UTC
Body I am be outside

Author Wu Chai (Facebook: 100007877380676)
Sent 2022-04-20 00:51:03 UTC

On Wednesday, October 19, 2022 CHOL's Facebook account publicly posted "If you got a credit union on for some time and u ready to get down to business hit me we'll both be happy by Friday for sure." See Exhibit 19 below.

Exhibit 19



Based on my training and experience, I know that online criminal actors, which include those involved in the use of stolen credentials, often recruit money launders to either move received fraudulent funds through domestic bank accounts or to withdraw the funds from the money launderers' bank account. Recruited money launderers often use a bank account in their own name or in the name of a fictitious or "sham" company that has no true business purpose. This practice helps to insulate the online criminal actors from law enforcement detection. Aged bank accounts have great value to an online criminal actor as financial institutions may scrutinize high value transactions made to newly opened bank accounts. I therefore believe, based on my training and experience, that in the Facebook post shown above, CHOL is recruiting money launderers who have an aged account, i.e., "a credit union on for some time."

On October 7, 2022 at approximately 7:44AM, CHOL's Facebook account publicly posted "Let's start off next week right swing all banks" to their Facebook account. See Exhibit 20 below.

Exhibit 20



Based on my training and experience, "swinging" a bank account can mean moving funds through a bank account rather than holding them in the bank account. If funds were held in a bank account, it is more likely that a financial institution could freeze the funds.

On October 7, 2022 at approximately 10:05AM, CHOL's Facebook account publicly posted "Who trying to make some bread hit me now" to their Facebook account. See Exhibit 21 below.

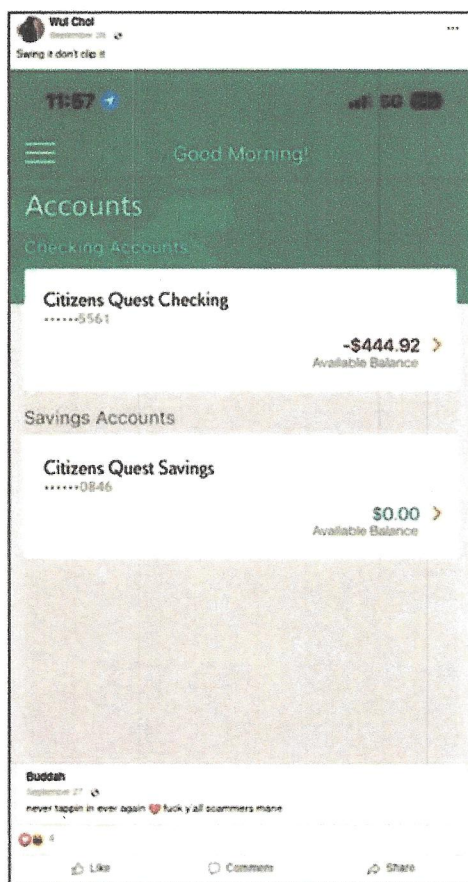
Exhibit 21



Based on my training and experience, I believe this post seeks others who are interested in earning money (i.e., "bread"). Read in conjunction with other posts on CHOL's Facebook account, I believe this post seeks others who are interested in earning money through illegal means.

On September 28, 2022, CHOL's Facebook account publicly replied to a Facebook post from Facebook user "Buddah." "Buddah" posted a screenshot of two bank accounts, one of which had a negative balance. "Buddah" wrote: "Never tappin ever again [heart emoji] fuck y'all scammers man." CHOL's Facebook account then responded to the text message by writing, "Swing it don't clip it". See Exhibit 22 below.

Exhibit 22



Based on my training and experience, I know that online criminal actors often communicate with recruited money launderers and co-conspirators over instant messaging and social media platforms, to

include Facebook. CHOL's Facebook account received "likes" and replies from other Facebook users to its Facebook posts, to include the message "Welcome" from Facebook user "Wun Junior Berrie" in reply to CHOL's Facebook account on October 19, 2022 post in Exhibit 19.



Pole camera surveillance conducted by FBI Buffalo showed that an individual matching CHOL's description entered and exited 20 Ferguson Ave multiple times on March 16, 2023. Physical surveillance conducted by FBI Buffalo on March 28, 2023 confirmed that CHOL is living at 20 Ferguson Ave. Additionally, on March 28, 2023 a United States Postal Inspection Service Operations Tech confirmed that CHOL was receiving mail at 20 Ferguson Ave.

Property records for 20 Ferguson Avenue, Buffalo, New York 14213 showed the residence was sold on April 21, 2010 to Berrie, Aniwang & Marial Isaac, who, according to open-source research, appear to be family members of CHOL.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

40. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what

tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times

and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a

computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

44. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described

in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

45. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature

called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and*

the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the

facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

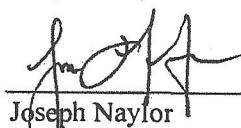
CONCLUSION

46. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

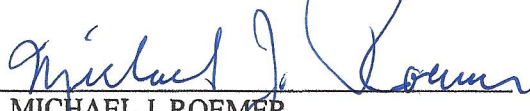
47. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



Joseph Naylor
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to, telephonically, this 3rd day of April,
2023.



HON. MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The property to be searched is 20 Ferguson Avenue, Buffalo, New York 14213, ("20 Ferguson") further described as a residential family structure. Property records for 20 Ferguson Avenue, Buffalo, New York 14213 showed the residence was sold on April 21, 2010 to Berrie, Aniwang & Marial Isaac.

The structure's front entrance faces south along Ferguson Avenue, has blue-colored exterior walls, a white front door with stairs up to the front porch, a second door on the residence's east side opens to the driveway on the east side of the residence.

The structure at 20 Ferguson does not appear to be marked with a house number. However, the structure to the east of 20 Ferguson is clearly marked with "22" on the left western-most post of the porch (as can be seen in the attached picture).





20 Ferguson Avenue

ATTACHMENT B

Property to Be Seized

1. All records relating to violations of Title 18, United States Code, Sections 1028(a)(7) (possession of means of identification in connection with another felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy), 1343 (Fraud by Wire), 1344 (Bank Fraud), 1349 (Wire Fraud and Bank Fraud Conspiracy), 1028A (Aggravated Identity Theft), 1956(a)(1)(A)(i) (Promotional Money Laundering), 1956(a)(1)(B)(i) (Concealment Money Laundering), 1957 (Transactional Money Laundering), 1956(h) (Money Laundering Conspiracy), 1030 (Computer Fraud and Abuse Act); 471 (Counterfeiting United States Currency); 473 (Buying, Selling, and Transferring Counterfeit United States Currency); Title 21, United States Code, Sections 844 (Simple Possession of Controlled Substances); 841(a)(1) (Distributing, Manufacturing, and Possessing with Intent to Distribute Controlled Substances); and 846 (Conspiracy to Violate 21 U.S.C. § 841(a)(1)) (the “Subject Offenses”), involving Wul Chol or Web Market A operators and occurring after March 1, 2020, including:
 - a. Drugs and drug paraphernalia, including illegal drugs and controlled substances;
 - b. Physical mediums related to bank or tax fraud, such as blank checks, paper, templates, dies, and ink;
 - c. Tools and other devices used, or which are capable of being used, to create or manufacture counterfeit currency, checks, money orders, and other monetary instruments
 - d. How-to guides related to malicious activity, including but not limited to bank accounts, tax filing, and credit cards;
 - e. Financial instruments and documents unrelated to occupants of the residence, including but not limited to bank checks, money orders, credit cards, and statements;

- f. Logs, books, address books, phone number books or other lists related to the tracking or facilitation of illegal activity;
 - g. Records and information relating to Web Market A;
 - h. Records and information relating to an access, use, possession, or control over stolen personal information, financial information, and/or electronic devices.
 - i. Records and information relating to cholw2016@yahoo.com;
 - j. Records and information relating to the identity or location of the suspect(s);
 - k. Records and information relating to malicious software;
 - l. Records and information relating to finances, including financial institutions, financial instruments,
 - m. Records and information relating to virtual currency such as bitcoin.
2. Computers or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
- a. the records identified in paragraph 1 of this Attachment B;
 - b. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- d. evidence of the lack of such malicious software;
 - e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - f. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - i. evidence of the times the COMPUTER was used;
 - j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - l. records of or information about Internet Protocol addresses used by the COMPUTER;
 - m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - n. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.